

## UNITED STATES DISTRICT COURT

SOUTHERN

DISTRICT OF

CALIFORNIA

FILED

08 MAR 21 PM 4:31

## In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

Sprint Samsung Cellular Telephone  
 Flip style phone  
 Serial #03215457966/20EBDEAE

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

BY:

DEPUTY

Case Number: 08MJ0622 KJS

'08 MJ 0896

I, Kevin J. Straus being duly sworn depose and say:I am a(n) Special Agent of the Federal Bureau of Investigation and have reason to believe

Official Title

that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

See Attachment A (incorporated by reference herein)

in the Southern District of California

there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment B (incorporated by reference herein)

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

fruits, instrumentalities and evidence

concerning a violation of Title 18 United States code, Section(s) 2113(a)

The facts to support a finding of probable cause are as follows:

See attached Affidavit of SA Kevin J. Strauss

Continued on the attached sheet and made a part hereof:

☒ Yes ☐ No

Kevin J. Straus  
 Signature of Affiant

Sworn to before me and subscribed in my presence,

Date MAR 21 2008

at

San Diego, California

City

State

LEO S. PAPAS  
U.S. MAGISTRATE JUDGE

Name of Judge

Title of Judge

Signature of Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

Sprint Samsung Cellular Telephone  
Flip style phone  
Serial #03215457966/20EBDEAE

currently in the possession of the Federal Bureau of Investigation Evidence Control  
Center in San Diego, CA.

ATTACHMENT B

ITEMS TO BE SEIZED:

1. The phone numbers and/or names and identities assigned to the cellular phone;
2. Digital, cellular, and/or telephone numbers, names and identities stored in the directories;
3. Phone numbers dialed from the cellular phone and stored in memory;
4. The last numbers dialed from the cellular phone;
5. The last numbers received to the cellular telephone;
6. Photographs stored in the memory of the cellular telephone,
7. Text messages sent and received from the cellular telephone, and;
8. Any other electronic information in the stored memory of the cellular phone, relating to violations of 18 U.S.C. 2113(3).

SOUTHERN DISTRICT OF CALIFORNIA

**AFFIDAVIT OF KEVIN J. STRAUSS**

I, Kevin J. Strauss, being duly sworn, depose and state the following:

1. I make this affidavit in support of an application for a search warrant in furtherance of a bank robbery investigation conducted by Special Agents of the Federal Bureau of Investigation and San Diego Police Department for the following target locations: one Sprint Samsung flip phone, serial number 03215457966/20EBDEAE with photo capabilities seized from Josiah Jorel Jackman; and one Notebook laptop computer, Model M54G "Alienware," serial number KA61N4N1N298 seized from Jackman's residence.

2. Based upon my experience and training, and all the facts and opinions set forth in this Affidavit, I believe items will be found in the cellular telephone and computer to be searched which evidences (1) the existence of the commission of, or conspiracy for the commission of, bank robbery in violation of 18 U.S.C. §2113(a), (2) contraband, fruits of crime or things otherwise criminally possessed, and (3) property designed or intended for use or which is or has been used as a means of committing criminal offenses. See Attachment B for list of items to be seized.

3. The information contained in this affidavit is based on my experience and training, consultation with other special agents of the Federal Bureau of Investigation (FBI), San Diego Police Department (SDPD), and other federal agents

1 and state law enforcement officers. The evidence and  
2 information contained herein was developed from interviews,  
3 documents, agency reports, and public records.

4 I.

5 **EXPERIENCE AND TRAINING**

6 4. I am a Special Agent (SA) with the Federal  
7 Bureau of Investigation (FBI). I have been employed by the  
8 FBI for approximately three years. I am currently assigned  
9 to the FBI Violent Crimes Squad, San Diego, California.

10 5. During my three years with the FBI, I have been  
11 involved in numerous investigations related to a wide variety  
12 of suspected criminal activity including narcotics  
13 trafficking, money laundering, bank robberies, kidnaping,  
14 assaults on federal officers, and murder-for-hire. Through  
15 my training, education and experience, I have become familiar  
16 with the methods of operation used by bank robbers. I am  
17 familiar with, and have participated in, all of the normal  
18 methods of investigation including, but not limited to,  
19 visual surveillance, questioning of witnesses, the use of  
20 search and arrest warrants, the use of confidential sources  
21 and informants, the use of pen registers, the use of court  
22 authorized wire intercepts, and the use of undercover agents.

23 II.

24 **DETAILS OF THE INVESTIGATION**

25 The following statements are based on my own  
26 investigation of the criminal activity described herein,  
27 investigation by other federal agents and local law  
28 enforcement officers, as well as my experience, training, and

1 background as a Special Agent with the FBI. Since this  
2 affidavit is submitted for a limited purpose, I have not  
3 included every fact I know about this investigation. I set  
4 forth only the facts necessary to establish foundation for  
5 the requested warrants.

6 6. On Friday, February 29, 2008, at approximately  
7 4:15 p.m., I responded to the report of a robbery at the Bank  
8 of America located at 7404 Jackson Drive, San Diego,  
9 California.

10 7. I interviewed the victim teller who advised as  
11 follows: On Friday, February 29, 2008, the victim teller  
12 was at her teller station when a lone male, later identified  
13 as JOSIAH JOREL JACKMAN, vaulted the teller counter top and  
14 loudly stated, "This is a robbery." JACKMAN ordered all  
15 three tellers working behind the counter at that time to open  
16 both their top and bottom cash drawers. JACKMAN grabbed  
17 stacks of cash out of the cash drawers one by one while  
18 repeatedly ordering the tellers to stand back. Within the  
19 money JACKMAN took were three concealed electronic tracking  
20 devices. Thereafter, he vaulted back over the counter and  
21 departed the bank. The teller described JACKMAN as a 6 foot  
22 male wearing a grey, long sleeved hooded sweatshirt, gloves,  
23 and a reddish cloth-type material over his face.

24 8. I learned the following from Officer Reichner,  
25 SDPD: On Friday, February 29, 2008, Officer Reichner and his  
26 partner responded to the report of a robbery at the Bank of  
27 America, 7404 Jackson Drive, San Diego, California. Officer  
28 Reichner was updated on JACKMAN's position based on the

1 signal received from the electronic tracking device JACKMAN  
2 took from the bank. At approximately 4:29 p.m. (almost 15  
3 minutes after the robbery), Officer Reichner and his partner  
4 found and detained JACKMAN while seated in a red Pontiac  
5 Grand Am. The vehicle was parked in a commercial area near  
6 6500 Riverdale Drive, San Diego, California. During an  
7 inventory search of the car incident to JACKMAN's arrest, a  
8 backpack with U.S. currency totaling \$32,486.00 was found on  
9 the front passenger side floor area. Included in that money  
10 were three concealed electronic tracking devices. Some of  
11 the money had spilled out of the backpack onto the car floor  
12 area. In the trash dumpster next to where JACKMAN was  
13 parked, the grey hooded sweatshirt and reddish cloth JACKMAN  
14 wore while robbing the bank were found. A witness from the  
15 bank, who had seen JACKMAN remove the red cloth from his face  
16 after exiting the bank, positively identified JACKMAN as the  
17 bank robber during a curbside lineup. Officer Reichner then  
18 transported JACKMAN to the SDPD Headquarters.

19 9. JACKMAN was searched by SDPD. Target cellular  
20 telephone was located on the person of JACKMAN in his pocket.  
21 The cellular telephone was seized and transported to the San  
22 Diego Division FBI Evidence Control Center where it is being  
23 secured.

24 10. On Friday, February 29, 2008, I interviewed  
25 JACKMAN at the SDPD Headquarters. After being advised of his  
26 Miranda Rights, JACKMAN voluntarily provided the following  
27 statement: On February 28 and 29, 2008, JACKMAN prepared for  
28 the bank robbery, i.e., he admitted to cutting a "beanie hat"

1 into a mask. In addition, JACKMAN stated that he drove his  
2 roommate, James Cook, to work so that he would have access to  
3 Cook's Pontiac Grand Am. On Friday, February 29, 2008,  
4 JACKMAN drove to an area near the Bank of America located at  
5 7404 Jackson Drive, San Diego, California and parked the  
6 Pontiac Grand Am. JACKMAN walked to a bench near the bank  
7 and watched the bank for several hours before entering.  
8 Thereafter, he entered the bank, vaulted the counter,  
9 announced that he was robbing the bank, and ordered all three  
10 tellers to open their top and bottom cash drawers. The  
11 victim tellers complied with JACKMAN's demands and JACKMAN  
12 proceeded to grab handfuls of cash from each open drawer.  
13 JACKMAN placed the loot from the teller drawers into a  
14 backpack he carried into the bank. Thereafter, JACKMAN  
15 vaulted back over the counter and fled the bank on foot with  
16 the cash. As JACKMAN departed the bank, he took off his  
17 cloth mask and ran to the Grand Am. JACKMAN departed the  
18 residential area, drove and parked in nearby commercial area.  
19 While in the Grand Am, JACKMAN was approached and detained by  
20 the police.

21 11. Also during his interview, JACKMAN was asked  
22 if he had ever discussed robbing banks with anyone before the  
23 Bank of America robbery. JACKMAN replied that he and his  
24 friends would often joke around about robbing banks. They  
25 would also go as far as to state how they would go about  
26 robbing a bank if they were to do it.

27 12. JACKMAN used a Pontiac Grand Am owned by his  
28 roommate, James Cook, on the day of the robbery.

13. At the end of the interview, JACKMAN gave



1 consent to the FBI and SDPD to search his premises,  
2 specifically his area/room, located at 6532 Reflection Drive,  
3 San Diego, California. A "Notebook" laptop computer (target  
4 computer) was located in the common area, i.e. living room  
5 table, of the apartment. JACKMAN's roommate, James Cook,  
6 identified the laptop as being JACKMAN's. Pursuant to the  
7 consensual search, JACKMAN's laptop computer was seized.

8 14. In addition, a Sony Cybershot 7.2 digital  
9 camera was discovered in JACKMAN's bedroom in his bedside  
10 dresser. A review of the photographs on the digital camera's  
11 memory revealed photographs of JACKMAN posing with large  
12 amounts of cash. The date stamp on the digital photographs  
13 indicate December 2007. A copy of some of the photographs  
14 have been attached to this affidavit. (See Exhibit 1 attached  
15 hereto.)

16 15. I assisted in the consent search of JACKMAN's  
17 apartment. After a review of the photographs, it appears as  
18 if the above referenced photographs (Exhibit 1) were taken  
19 inside JACKMAN's apartment located at 6532 Reflection Drive,  
20 San Diego, California.

### 21 III.

#### 22 BASIS FOR EVIDENCE SOUGHT IN SEARCH WARRANTS

23 16. Through my training and experience, and in  
24 consultation with other agents and informants, I have learned  
25 that:

26 a. Bank robbers may communicate via cellular  
27 telephones and store the names and telephone numbers of other  
28 people involved in bank robberies in the memory of the  
cellular telephones.

1           b. Bank robbers may utilize cellular telephones  
2 with photo capabilities to take photographs and videos of co-  
3 conspirators, money, assets purchased with bank robbery  
4 proceeds, and targeted banks.

5           c. Bank robbers may utilize the text or email  
6 functions on cellular telephones in the planning and/or  
7 commission of the crime.

8           d. Bank robbers may utilize computers in the  
9 preparation, planning, and organization of bank robberies  
10 including use of e-mail to communicate with co-conspirators;  
11 creation of bank robbery plans; creation of bank robbery  
12 notes; storage of photographs and videos of co-conspirators,  
13 money, assets purchased with bank robbery proceeds, and  
14 targeted banks; internet searches for identification of  
15 targeted bank; internet searches for identification of get-a-  
16 way routes such as "mapquest"; and storage of financial data  
17 related to bank robbery proceeds.

18           17. JACKMAN admitted that he spent at least two  
19 hours on a bench watching the bank prior to robbing it.  
20 Based on my training and experience, bank robbers often spend  
21 time surveilling or "casing" banks prior to committing a  
22 robbery. Based on my training and experience, I believe it  
23 is possible that JACKMAN used his cellular telephone to  
24 communicate with others, either by telephone call or text  
25 message, prior to robbing the bank. In addition, it is  
26 possible that JACKMAN used his cellular telephone to take  
27 photographs in preparation for the commission of the bank  
28 robbery. This information and evidence may be stored on the  
phone's memory.

## COMPUTER SEARCH PROTOCOL

# Forensic Imaging

8

1 commission of the enumerated offenses will be returned to its  
2 owner. For computers that are retained, the owner may apply  
3 in writing to the undersigned for return of specific data not  
4 otherwise subject to seizure for which the owner has a  
5 specific need. The [seizing agency] will reply in writing.  
6 In the event that the owner's request is granted,  
7 arrangements will be made for a copy of the requested data to  
8 be obtained by the owner. If the request is denied, the  
9 owner will be directed to Rule 41(g), Federal Rules of  
10 Criminal Procedure.

11           b. A forensic image is an exact physical copy of  
12 the hard drive or other media. It is essential that a  
13 forensic image be obtained prior to conducting any search of  
14 the data for information subject to seizure pursuant to this  
15 warrant. A forensic image captures all of the data on the  
16 hard drive or other media without the data being viewed and  
17 without changing the data in any way. This is in sharp  
18 contrast to what transpires when a computer running the  
19 common Windows operating system is started, if only to peruse  
20 and copy data - data is irretrievably changed and lost. Here  
21 is why: When a Windows computer is started, the operating  
22 system proceeds to write hundreds of new files about its  
23 status and operating environment. These new files may be  
24 written to places on the hard drive that may contain deleted  
25 or other remnant data. That data, if overwritten, is lost  
26 permanently. In addition, every time a file is accessed,  
27 unless the access is done by trained professionals using  
28 special equipment, methods and software, the operating system  
will re-write the metadata for that file. Metadata is

1 information about a file that the computer uses to manage  
2 information. If an agent merely opens a file to look at it,  
3 Windows will overwrite the metadata which previously  
4 reflected the last time the file was accessed. The lost  
5 information may be critical.

6 c. Special software, methodology and equipment is  
7 used to obtain forensic images. Among other things, forensic  
8 images normally are "hashed," that is, subjected to a  
9 mathematical algorithm to the granularity of 1038 power, an  
10 incredibly large number much more accurate than the best DNA  
11 testing available today. The resulting number, known as a  
12 "hash value" confirms that the forensic image is an exact  
13 copy of the original and also serves to protect the integrity  
14 of the image in perpetuity. Any change, no matter how small,  
15 to the forensic image will affect the hash value so that the  
16 image can no longer be verified as a true copy.

#### 17 Forensic Analysis

18 d. After obtaining a forensic image, the data will  
19 be analyzed. Analysis of the data following the creation of  
20 the forensic image is a highly technical process that  
21 requires specific expertise, equipment and software. There  
22 are literally thousands of different hardware items and  
23 software programs that can be commercially purchased,  
24 installed and custom-configured on a user's computer system.  
25 Computers are easily customized by their users. Even  
26 apparently identical computers in an office environment can  
27 be significantly different with respect to configuration,  
28 including permissions and access rights, passwords, data  
storage and security. It is not unusual for a computer

1 forensic examiner to have to obtain specialized hardware or  
2 software, and train with it, in order to view and analyze  
3 imaged data.

4 e. Analyzing the contents of a computer, in  
5 addition to requiring special technical skills, equipment and  
6 software also can be very tedious. It can take days to  
7 properly search a single hard drive for specific data.  
8 Searching by keywords, for example, often yields many  
9 thousands of "hits," each of which must be reviewed in its  
10 context by the examiner to determine whether the data is  
11 within the scope of the warrant. Merely finding a relevant  
12 "hit" does not end the review process. As mentioned above,  
13 the computer may have stored information about the data at  
14 issue: who created it, when it was created, when was it last  
15 accessed, when was it last modified, when was it last printed  
16 and when it was deleted. Sometimes it is possible to recover  
17 an entire document that never was saved to the hard drive if  
18 the document was printed. Operation of the computer by  
19 non-forensic technicians effectively destroys this and other  
20 trace evidence. Moreover, certain file formats do not lend  
21 themselves to keyword searches. Keywords search text. Many  
22 common electronic mail, database and spreadsheet applications  
23 do not store data as searchable text. The data is saved in a  
24 proprietary non-text format. Microsoft Outlook data is an  
25 example of a commonly used program which stores data in a  
26 non-textual, proprietary manner-ordinary keyword searches  
27 will not reach this data. Documents printed by the computer,  
28 even if the document never was saved to the hard drive, are  
recoverable by forensic examiners but not discoverable by

1 keyword searches because the printed document is stored by  
2 the computer as a graphic image and not as text. Similarly,  
3 faxes sent to the computer are stored as graphic images and  
4 not as text.

5 f. Analyzing data on-site has become increasingly  
6 impossible as the volume of data stored on a typical computer  
7 system has become mind-boggling. For example, a single  
8 megabyte of storage space is the equivalent of 500  
9 double-spaced pages of text. A single gigabyte of storage  
10 space, or 1,000 megabytes, is the equivalent of 500,000  
11 double-spaced pages of text. Computer hard drives are now  
12 capable of storing more than 100 gigabytes of data and are  
13 commonplace in new desktop computers. And, this data may be  
14 stored in a variety of formats or encrypted. The sheer  
15 volume of data also has extended the time that it takes to  
16 analyze data in a laboratory. Running keyword searches takes  
17 longer and results in more hits that must be individually  
18 examined for relevance. Even perusing file structures can be  
19 laborious if the user is well-organized. Producing only a  
20 directory listing of a home computer can result in thousands  
21 of pages of printed material most of which likely will be of  
22 limited probative value.

23 g. Based on the foregoing, searching any computer  
24 or forensic image for the information subject to seizure  
25 pursuant to this warrant may require a range of data analysis  
26 techniques and may take weeks or even months. Keywords need  
27 to be modified continuously based upon the results obtained;  
28 criminals can mislabel and hide files and directories, use  
codes to avoid using keywords, encrypt files, deliberately

1 misspell certain words, delete files and take other steps to  
2 defeat law enforcement. In light of these difficulties, your  
3 affiant requests permission to use whatever data analysis  
4 techniques reasonably appear necessary to locate and retrieve  
5 digital evidence within the scope of this warrant.

6 h. All forensic analysis of the imaged data will  
7 be directed exclusively to the identification and seizure of  
8 information within the scope of this warrant.

9 V.

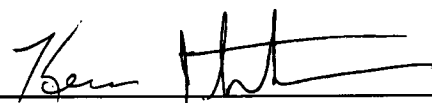
10 CONCLUSION

11 20. Based on my training and experience,  
12 consultation with other special agents and law enforcement  
13 officers, and all of the facts and opinions set forth in this  
14 affidavit, I have probable cause to believe that violations  
15 of 18 U.S.C. §2113(a) - bank robbery, have been committed and  
16 evidence of the crimes will be found in the cellular  
17 telephone and computer seized from JACKMAN (as described in  
18 Attachment A of each search warrant). I believe that  
19 evidence of other co-conspirators involved in, and associated  
20 with, bank robbery, as well as evidence of the commission of  
21 bank robberies will be found on the cellular telephone and  
22 computer seized from Jackman.



21. Wherefore, your affiant respectfully requests  
a warrant be issued authorizing FBI Special Agents and task  
force officers to examine, analyze, and make record of the  
contents of the information stored in the seized cellular  
telephone and computer as described in Attachment A of each  
search warrant.

Executed on March 20, 2008, at 405 p.m.

  
Kevin J. Strauss  
Special Agent, FBI

Sworn to and subscribed before me  
this 21<sup>st</sup> day of March, 2008

  
LEO S. PAPAS  
United States Magistrate Judge

**MAR 21 2008** 405 PM  
Date/Time

# **EXHIBIT 1**



(Photos Taken Dec 2007)

